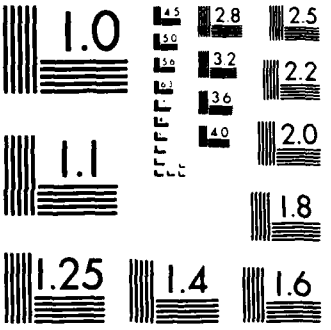
AD-A185 883 SHORT PSEUDORANDOM TEST SEQUENCES(U) STANFORD UNIV CA 1/1
CENTER FOR RELIABLE COMPUTING E J MCCLUSKEY ET AL.
FEB 87 CRC-TR-87-6 N00014-85-K-0600

UNCLASSIFIED F/G 12/3 NL



DTIC FILE COPY

SECURITY CLASSIFICATION

AD-A185 883

TATION PAGE

1a REPORT SECURITY CLA UNCLASSIFIED	RESTRICTIVE MARKINGS NA
2a SECURITY CLASSIFICATION AUTHORITY NA	3 DISTRIBUTION/AVAILABILITY OF REPORT Approved for public release; distribution unlimited
2b DECLASSIFICATION/DOWNGRADING SCHEDULE NA	
4 PERFORMING ORGANIZATION REPORT NUMBER(S) CRC-87-6 (CSL TN 87-321	5 MONITORING ORGANIZATION REPORT NUMBER(S) N00014-85-K-0600
6a NAME OF PERFORMING ORGANIZATION Center for Reliable Computing	6b OFFICE SYMBOL (If applicable)
6c ADDRESS (City, State, and ZIP Code) ERL 460 Stanford University Stanford, CA 94305-4055	7a NAME OF MONITORING ORGANIZATION Resident Representative, ONR
	7b ADDRESS (City, State, and ZIP Code) Durand 165 Stanford University Stanford, CA 94305-2192
8a NAME OF FUNDING/SPONSORING ORGANIZATION ONR	8b OFFICE SYMBOL (If applicable)
	9 PROCUREMENT INSTRUMENT IDENTIFICATION NUMBER 2 DPN540
8c ADDRESS (City, State, and ZIP Code) Detachment, Pasadena 1030 E. Green St. Pasadena, CA 91106-2485	10 SOURCE OF FUNDING NUMBERS PROGRAM ELEMENT NO / PROJECT NO / TASK NO. / WORK UNIT ACCESSION NO

11 TITLE (Include Security Classification)

Short Pseudorandom Test Sequences

12 PERSONAL AUTHOR(S)
E.J. McCluskey and K.D. Wagner

13a TYPE OF REPORT	13b TIME COVERED	14 DATE OF REPORT (Year, Month, Day)	15 PAGE COUNT
Technical Report	FROM _____ TO _____	February 1987	11

16 SUPPLEMENTARY NOTATION

17 COSATI CODES			18 SUBJECT TERMS (Continue on reverse if necessary and identify by block number)
FIELD	GROUP	SUB-GROUP	

19 ABSTRACT (Continue on reverse if necessary and identify by block number)

This paper presents a probabilistic model for pseudorandom testing of combinational circuits and shows how the general model can be simplified for short test sequences.

20 DISTRIBUTION/AVAILABILITY OF ABSTRACT	21 ABSTRACT SECURITY CLASSIFICATION	
☒ UNCLASSIFIED/UNLIMITED ☐ SAME AS RPT ☐ DTIC USERS		
22a NAME OF RESPONSIBLE INDIVIDUAL E.J. McCluskey	22b TELEPHONE (Include Area Code) 415/723-1451	22c. OFFICE SYMBOL

Center for Reliable Computing

Short Pseudorandom Test Sequences

E.J. McCluskey and K.D. Wagner

CRC Technical Report No. 87-6

(CSL TN No. 87-321)

February 1987

CENTER FOR RELIABLE COMPUTING

Computer Systems Laboratory
Electrical Engineering and Computer Science Departments
Stanford University, Stanford, CA

ABSTRACT

This paper presents a probabilistic model for pseudorandom testing of combinational circuits and shows how the general model can be simplified for short test sequences.

Imprimatur: I. Shperling and J.G. Udell Jr.

This report was supported by the Innovative Science and Technology Office of the Strategic Defense Initiative Organization and administered through the Office of Naval Research under Contract No. N00014-85-K-0600.

SHORT PSEUDORANDOM TEST SEQUENCES

E.J. McCluskey and K.D. Wagner

CENTER FOR RELIABLE COMPUTING
Computer Systems Laboratory
Departments of Computer Science and Electrical Engineering, Stanford University,
Stanford, CA 94305-4055 USA

ABSTRACT

This paper presents a probabilistic model for pseudorandom testing of combinational circuits and shows how the general model can be simplified for short test sequences.

INTRODUCTION

Pseudorandom test pattern generation uses an autonomous linear feedback shift register, ALFSR, as a source of test vectors. These test vectors can be, and are, used to test both combinational and sequential networks. Sequential circuit pseudorandom testing is discussed in [Losq 78].

Only combinational circuit testing is considered here. This discussion applies mainly to on-line testing in which the test patterns are generated during the test procedure rather than being stored copies of previously generated patterns. The difference is that all of the first L vectors in the sequence must be used rather than selected patterns. The patterns may be generated by circuits or by a program simulating an ALFSR.

The major current issues for pseudorandom test pattern generation are: selecting the test length, determining the fault coverage, and identifying "random-pattern resistant" faults (faults that are hard-to-detect with random patterns). These could, in principle, all be accomplished by a full single-stuck fault simulation of the network to be tested. The development of special purpose equipment is decreasing the cost of fault simulation. Despite this cost reduction, full fault simulation remains prohibitively expensive for modern large networks that require long pseudorandom test sequences for adequate fault coverage. The only viable alternative to full fault simulation appears to be the use of a probabilistic model of pseudorandom test pattern generation. This is the approach taken here.

Probabilistic modeling of pseudorandom test pattern generation was first proposed in [Rault 71] and has recently become an area of intense study. In [Shedletsky 77] and most of the subsequent work, pseudorandom test pattern generation is modeled as a random process. This random model corresponds to "sampling with replacement" and each input pattern always has the same probability of occurring. This does not account for the fact that patterns generated by an ALFSR do not repeat until all of the non-zero patterns occur. the term "pseudorandom," rather than random, is often used to describe this non-repeating characteristic of ALFSR patterns. A pseudorandom process corresponds to "sampling without replacement", the model used here. The results obtained using a pseudorandom model are compared to those based on a random model. For short test sequences the results for these two models do not differ significantly.

Exhaustive (all possible) input patterns are as easy to generate as pseudorandom patterns. In fact, a simple modification converts an ALFSR to an exhaustive test pattern generator, [McCluskey 86]. Exhaustive test patterns do not require any fault simulation or coverage estimation. Pseudorandom patterns should be used only when an exhaustive test is too long. It thus is reasonable to assume that the length of a pseudorandom test is much shorter than an exhaustive test. This assumption will be used to simplify the models developed here. Most of the results thus apply only to short pseudorandom tests, a concept that will be quantized below. The restriction to short pseudorandom tests is not a significant drawback since these are the only practical pseudorandom tests.

Networks that require exhaustive test patterns (all possible inputs) for high fault coverage are possible. Thus, some attribute of the particular network under test must be taken into consideration in determining a practical pseudorandom test. The network attribute most relevant to pseudorandom testing appears to be the fault detectability profile introduced in [Malaiya 84]. The *detectability*, k, of a fault is the number of network input patterns that cause that fault to be detected. The *fault detectability profile* is the set of detectabilities for all single-stuck faults in the network. There is no reason that other types of faults could not be considered as well. In an attempt to simplify the analysis, [Shedletsky 77] suggested that only the "worst case" fault be considered. (Although [Shedletsky 77] didn't use this terminology, the worst case fault corresponds to the fault with the smallest detectability.) The inadequacy of this approach is demonstrated in [Wagner 87]. A precise characterization of the minimum set of fault detectabilities that must be considered is derived here.

The test patterns can be applied to the network-under-test (NUT) either by connecting the parallel outputs of the ALFSR directly to the network inputs or by shifting the serial output of the ALFSR into the scan path bistables that connect to the network inputs. In either structure the number of ALFSR stages need not be the same as the number of network inputs. The general case of different numbers of inputs and stages is considered here. It will be demonstrated that the same formulas apply to all situations in which the number of ALFSR stages isn't smaller than the number of network inputs.

A model for the escape probability of a fault is derived and simplified for faults with small detectability. The assumption that only faults with low detectabilities need be considered is justified by demonstrating that these are the only faults that are significant in calculating the expected fault coverage of a pseudorandom test.

The assumption of short test lengths is then used to further simplifiy the escape probability expressions, which are then used in formulas for the expected fault coverage of a pseudorandom test of length L. The concept of a random-pattern resistant fault is quantized.

ESCAPE PROBABILITY

The major results in this section are expressions for the probability that a fault of a specific detectability is not detected by a pseudorandom test.

DEFINITION: A *pseudorandom test sequence* is a sequence of L m-bit binary patterns that are the consecutive states of some m bit ALFSR. In the analysis here, these will be modeled as sequences of m-bit patterns chosen randomly, without replacement and with equal probability, from the set of all $M = 2^m - 1$ non-zero m-bit patterns. The all-0 pattern is excluded because it does not occur in an ALFSR.

DEFINITION: A *pseudorandom test* is the application of a pseudorandom test sequence to the network under test, NUT, and the observation of the resulting network outputs. The NUT is assumed to be combinational with n inputs so that the total number of possible input patterns is $N = 2^n$.

DEFINITION: The *detectability*, k, of a fault is the number of network input patterns that cause that fault to be detected (because at least one network output with the fault present differs from the output without the fault).

For a network consisting of a single 3-input AND Gate, a stuck-at-1 fault on an input lead has k=1, while k=7 for the stuck-at-1 fault on the output lead.

Another useful parameter when the number of ALFSR stages differs from the number of circuit inputs is the test source detectability, K.

DEFINITION: The test source *detectability, K*, of a fault is the number of ALFSR contents that cause that fault to be detected for a particular test setup.

The detectability k depends only on the network, while the test source detectability, K, is a function of both the network and the particular test arrangement. For example, consider a network N made up of a single 3-input AND Gate. The stuck-at-0 fault on the gate output is detected only by the (1 1 1) input pattern, thus k for this fault is 1. If a 3-stage ALFSR is used to test N, K is also 1. On the other hand, if a 5-stage ALFSR with outputs from 3 of the stages connected to the network inputs is used, K = 4, since there are 4 ALFSR contents that produce network inputs that detect the fault.

DEFINITION: The *escape probabilities* Q_k *and* Q_K, are the probabilities that a fault of detectability k and test source detectability K is not detected.

THEOREM 1: For a pseudorandom test the escape probability is given by:

$$Q_K = \frac{\binom{M-L}{K}}{\binom{M}{K}} \qquad (1)$$

which can also be written as:

$$Q_K = \prod(1 - L / (M+1 - j)) \qquad \text{for } j = 1 \text{ to } K \qquad (2)$$

These equations can be simplified to the following bounds which are excellent approximations to Q_K for useful numerical values of the parameters in the expressions.

$$(1 - L / (M-K))^K \quad < Q_K \leq \quad (1 - L / M)^K \qquad (3)$$

$$Q_K \leq \quad e^{- KL / M} \qquad (4)$$

PROOF: Equation (1) is simply the ratio of the number of ways to choose K positions for the detecting patterns from the last M-L positions in the ALFSR output sequence that are not used as test vectors divided by the number of ways to choose K positions from the entire ALFSR output sequence. A somewhat more complex derivation of a similar result for the case when m=n is presented in [Wagner 87] where it occurs in equation (8).

Equation (2) is derived by writing out the binomial coefficients in equation (1), cancelling common factors, and dividing each factor by M. Inequality (3) results from replacing j by K+1 in each factor to obtain the lower bound and replacing j by 1 in each factor to obtain the upper bound. These bounds are very tight for values of K that are small compared to M. Detectabilities that are not small compared to M correspond to faults that are easily detected. Such easily detected faults will be shown to have a negligible effect on the expected fault coverage. The bounds are thus very good for the hard-to-detect faults which are the main items studied here.

Inequality (4) is derived from the general inequality $\ln(z) \leq z-1$. This is proved on page 23 of [Gallager 68]. Replacing z by $1- L/M$ gives $\ln(1-L/M) \leq -L/M$, multiplying both sides by K gives $K \ln(1-L/M) \leq -K(L/M)$, and taking the antilogarithm of both sides gives $(1 - L/M)^K \leq e^{- KL/M}$. The equality $\ln(L/M) = L/M - 1$ is true only when $L/M = 0$, but the difference between the two sides is small for small L/M.

A drawback of the expressions of Theorem 1 is their dependence on a particular test arrangement rather than on only the network being tested. The following theorem presents expressions for the escape probability that are based on N and k. First, lemmas relating N and k to M and K will be derived.

Lemma 1: When $m = n$, $M = N-1$ and $K = k$ or $k-1$. Since pseudorandom testing is only required for networks with $N >> 1$, there is little loss in assuming that $M = N$. Whether $K = k$ or $k-1$ depends on whether the all-0 pattern is one of the k patterns that detect the fault in question. As will become obvious in the discussion of numerical values of the parameters, unless $k >> 1$ the corresponding fault is very likely to go undetected by a pure pseudorandom test. Thus, it will be assumed that $K = k$.

Lemma 2: When $m > n$ ($m = n + r, r \geq 1$), $M = 2^r 2^n - 1$ and $N = 2^n$. Thus, $M = 2^r N - 1$ and $K = 2^r k$ or $2^r k - 1$. Similar reasons to those given in lemma 1 permit the 1s to be dropped, giving $M = 2^r N$ and $K = 2^r k$.

Lemma 3: When $m < n$ ($m = n - r, r \geq 1$), $M = 2^{-r} 2^n - 1$ and $N = 2^n$. M is smaller than N, but must still be large compared to 1 so that it can be very accurately approximated by $M = 2^{-r}N$. A simple structure for this situation has a test pattern generator consisting of an m-stage ALFSR with the output of the last stage used as the input of an r-stage shift register. The structure consisting of the ALFSR and the shift register will be called an *extended register*. The n network inputs are taken from the $n = m + r$ outputs of the extended register. Two types of faults must be considered:

(1) faults for which all of the network input patterns that detect the faults come from a subset of the extended register outputs that contains at most m contiguous stages. It is easy to show that any subset of m contiguous stages will contain all possible $2^m - 1$ non-zero binary patterns during one complete cycle of the ALFSR. For such faults, $K = k$ or $k-1$. As discussed in Lemma 1, it will be assumed that $K = k$.

(2) faults for which at least one of the network input patterns that detects the faults comes from a subset of the extended register outputs that contains more than n contiguous stages. A network input pattern derived from more than m continuous extended register stages may or may not appear in the extended register. Thus for faults of this type $K \leq k$.

The results of Lemmas 1-3 are summarized in Table 1.

Table 1. Relations between K and k and between M and N, assuming $M >> 1$, $k >> 1$.

$m = n$	$M = N$	$K = k$
$n < m = n + r, r \geq 1$	$M = 2^r N$	$K = 2^r k$
$n > m = n - r, r \geq 1$	$M = 2^{-r} N$	$K \leq k$

THEOREM 2: When $m \geq n$, expression (4) can be restated in terms of k and N.

$$Q_k \leq e^{-kL/N} \qquad \text{for } m \geq n \qquad (5)$$

Expression (5) is derived by substituting the values from Table 1 into expression (4) and cancelling common factors. Its advantage over expression (4) is that it depends only on the network under test and not the particular test structure. For the case where $m \leq n$, it is still necessary to use expression (4) since the escape probability is very dependent on the actual test structure.

It is interesting to note that if a random source of input patterns is assumed rather than a pseudorandom source the escape probability is given by:

$$Q_k = (1 - k/N)^L \leq e^{-kL/N} \qquad (6)$$

Each input pattern has a probability of k/N of detecting the fault so that the probability of L patterns not detecting the fault is given by $(1 - k/N)^L$. The inequality in (6) is derived by the same technique used for expression (4). The sameness of expressions (6) and (5) explains why some of the earlier papers on pseudorandom testing obtained valid results even though they use a random model rather than the more correct pseudorandom model.

FAULT COVERAGE

The quality of a test procedure is usually expressed in terms of the *single-stuck fault coverage*, the percentage of all single-stuck faults detected. Single-stuck faults are used because their use in the past has produced valuable results and they are the only type of faults for which reasonable computation procedures have been developed. In fact, they are so common that the qualifier is often dropped and the term fault coverage is used to mean single-stuck fault coverage. The techniques developed here are more general and the single-stuck fault assumption will only be required when techniques for computing the fault detectabilities k and K are discussed.

By using the expressions developed for the escape probability, it is straightforward to obtain expressions for the *expected fault coverage, E(C)*:

$$E(C) = 1 - 1/n_f \sum h_k Q_k$$

$$\geq 1 - 1/n_f \sum h_k e^{-kL/N} \qquad \text{for } m \geq n, \qquad 1 \leq k \leq N-L$$

$$\geq 1 - 1/n_f \sum h_K e^{-kL/M} \qquad \text{for } m < n, \qquad 1 \leq K \leq M-L$$

n_f = number of possible faults

h_k =number of faults with detectability k

h_K =number of faults with test source detectability K

It is often convenient to calculate the expected number of undetected faults:

$$E(U) = 1 - E(C) = 1/n_f \sum h_k Q_k$$

The relative contributions of the faults with different detectabilities can be made more explicit by rewriting this expression in terms of the minimum-detectability fault. The details are shown only for $m \geq n$, but similar results apply when $m < n$.

DEFINITION: Let

g be the minimum value of detectability k,

$q = e^{-gL/N}$, the escape probability of a fault with this lowest value of k, and

g_k be k/g, the normalized detectability. Thus: $k = g_k g$

Numerical values for these quantities for the '181 ALU are given in Table 2.

The expression for E(U) then can be written in terms of the normalized detectabilities as:

$$E(U) = 1/n_f \sum h_k e^{-kL/N} = 1/n_f \sum h_k (e^{-gL/N})^{g_k} = 1/n_f \sum h_k (q)^{g_k}, \qquad m \geq n$$

This expression shows that if the escape probability q for the lowest detectability fault is small, the escape probabilities for higher detectability faults will be exponentially lower. In spite of this, if some of the q_k are only slightly greater than one, they will still have a significant effect on E(U). The same conclusion is valid if some of the higher detectability faults have large values of h_k.

RANDOM PATTERN RESISTANT FAULTS

The concept of a "random pattern resistant" fault was introduced in [Eichelberger 83] which discusses the possibility that there are faults that are difficult to detect with a pseudorandom test. A mathematical characterization of such a fault is one with a low probability of detection or equivalently a large Q_k. This can be caused by a low detectability k or by a low test source detectability K due to a loss of detectability when the number of network inputs n is larger than the number of ALFSR stages. It is also possible that the lowest detectability is not alone sufficient to cause a significant loss of fault coverage, but there are very many faults with this lowest detectability so that taken together they produce a low value of coverage.

A more quantitative characterization results from assuming that:
(1) A "random pattern resistant" fault is one for which the escape probability is more than one half, and
(2) The pseudorandom test length is $L = 2^{20}$.
This test length corresponds to slightly more than one million test vectors which seems a reasonable upper bound on a practical test length. It follows from these assumptions that:

$$Q_k > 1/2 \text{ or } e^{-kL/N} > 1/2 \qquad \text{so that}$$

$$kL/N < \ln 2, \qquad k/N < (\ln 2)/2^{20} = 6.6 \times 10^{-7}$$

so that a random pattern resistant fault is one for which

$$k < 6.6N \times 10^{-7}$$

SOME NUMERICAL EXAMPLES

This section presents some data from published studies of pseudorandom testing. The major purpose is to put into perspective the assumptions that have been made about the relative parameter values. The circuit considered first is the '181 ALU. This circuit has been used extensively in testing studies because it was the most complex of the common standard combinational parts. Since the ALU has only 14 inputs, pseudorandom testing is not required since exhaustive testing is feasible. This ALU is too small to be a good example for pseudorandom test. In spite of this, it is probably the circuit for which most data is available which is why it is included here. In particular, the complete fault detectability profile for the ALU has been computed by exhaustive simulation of all single-stuck faults, [Wagner 87].

Calculation of the detectability profile. For circuits so large that pseudorandom testing is required, it clearly isn't feasible to find the detectability profile by exhaustive simulation. This has caused some skepticism about using the detectabilities to study pseudorandom testing. As will be demonstrated in the following, the complete detectability profile isn't required for useful results. A method has been developed for deriving the detectabilities that can find the smaller detectabilities without having to obtain the entire profile. This method does not require exhaustive simulation. It is a generalization of the

profile. This method does not require exhaustive simulation. It is a generalization of the approach described in [Illman 85], and is based on the use of circuit cones and segments. The detectability profile of the '181 ALU has been derived by hand using this method. A paper describing this method is currently being prepared.

Data for the '181 ALU. Table 2 shows the relevant parameters for the ALU. The detectabilities shown are the seven smallest values. Simulation was used in [Chin 87] to derive the expected fault coverage, $E(1- Q_k)$, for the fault with the lowest detectability (96).

Table 2. Parameters of the '181 ALU

n	14	..					
N	16,364						
n_f	400						
k	96	128	176	192	216	256	264
h_k	1	1	1	7	1	2	1
g	96						
g_k	1	1.33	1.833	2	2.25	2.69	2.75

The results of this study are shown in Table 3 along with the theoretical estimates using $Q_k \approx e^{-96\,L/N}$ based on expression (6).

Table 3 Estimated Expected Coverage for the Detectability-96 ALU Fault.

	Simulation Data		Theoretical Values
L	L/N	$E(1- Q_k)$	$1 - e^{-96\,L/N}$
136	0.0083	0.581	0.549
272	0.0166	0.829	0.797
320	0.0195	0.874	0.847
388	0.024	0.921	0.900
502	0.031	0.968	0.949
766	0.047	1.00	0.989

The differences between the simulated values and the theoretical values are due to the fact that the test lengths studied are not as short as assumed in the approximations used. As shown in the following section, test lengths for actual pseudorandom tests are much shorter than those used for the ALU.

Data for the Brglez Benchmark Circuits. A set of 10 circuits was proposed in [Brglez 85] for use as testing benchmarks. Another paper at the same conference, [Carter 85], reports the results of pseudorandom simulations of the Brglez circuits. In these circuits n, the number of inputs ranges from 32 to 233. Table 4 summarizes the simulation data from

this paper. The normalized test length (L/N) ranges from 2^{-20} to 2^{-212} which justifies the assumption that L << N.

Table 4. Simulation Data for the Brglez Circuits

Circuit	C432	C499	C880	C1355	C1908	C2670	C3540	C5315	C6288	C7522
Coverage	99.23	98.94	100	99.49	99.52	95.29	96.00	98.89	99.56	97.40
n	36	41	60	41	33	233	50	178	32	207
Test L	2^{11}	2^{12}	2^{14}	2^{12}	2^{13}	2^{21}	2^{15}	2^{13}	2^{8}	2^{21}
L/N	2^{-25}	2^{-29}	2^{-42}	2^{-29}	2^{-20}	2^{-212}	2^{-35}	2^{165}	2^{-24}	2^{-186}

SUMMARY AND CONCLUSIONS

Accurate approximations for the escape probability of a fault during pseudorandom testing have been developed with particular emphasis on the situation where the test length is a very small fraction of the total number of possible network input patterns. The normalized test length can be determined by assuming a value of the actual test length based on the amount of time that can be devoted to testing, for example $L = 2^{20}$. Based on the number of circuit inputs n, it is then possible to use the expression, $Q_k \approx e^{-k\,L/N}$ to estimate the minimum acceptable value for k. The network must then be analyzed to determine whether faults with lower values of k are possible. If this is true, modification of the network as discussed in [Eichelberger 83] must be considered. A technique for estimating the k's will be described in a paper under preparation. It should be pointed out that if there are only a few faults with unacceptably low k values, it may be possible to use an initial seed state in the ALFSR to eliminate the possibility that they aren't detected.

REFERENCES

[Brglez 85] Brglez, F., P. Pownall, and R. Hum, "Accelerated ATPG and Fault Grading via Testability Analysis," *Proc., Int'l Symp. Circuits and Systems, (ISCAS)*, pp. 695-698, Kyoto, Japan, June 1985.

[Carter 85] Carter, J.L., S.F. Dennis, V.S. Iyengar, and B.K. Rosen, "ATPG via Random Pattern Simulation," *Proc., Int'l Symp. Circuits and Systems, (ISCAS)*, pp. 683-686, Kyoto, Japan, June 1985.

[Chin 87] Chin, C.K., and E.J. McCluskey, "Test Length for Pseudorandom Testing," *IEEE Trans. Comput.* Vol. C-36, No. 2, pp. 252-256, Feb. 1987.

[Eichelberger 83] Eichelberger, E., and E. Lindbloom, "Random-Pattern Coverage Enhancement and Diagnosis for LSSD Logic Self-Test," IBM *j. res. develop.*, Vol. 27, No. 3, pp. 265-272, May 1983.

[Illman 85] Illman, R.J.,"Self-Tested Data Flow Logic: A New Approach," pp. 50-58, *IEEE Design and Test*, April 1985.

[Gallager 68] Gallager, R.G., "Information Theory and Reliable Communication," *John Wiley & Sons, Inc.*, New York, 1968.

[Losq 78] Losq, J., "Efficiency of Random Compact Testing," *IEEE Trans. Comp.*, Vol. C-27, No. 6, pp. 516-525, June 1978.

[Malaiya 84] Malaiya, Y.K. and S.Yang, "The Coverage Problem for Random Testing," *Proc., IEEE Int'l Test Conf.*, pp. 237-245, Nov. 1984.

[McCluskey 86] McCluskey, E.J., "Logic Design Principles with Emphasis on Testable

Semicustom Circuits," *Prentice-Hall, Inc.*, Englewood Cliffs, NJ, 1986.
[Rault 71] Rault, J.C., "A Graph Theoretical and Probabilistic Approach to the Fault Detection of Digital Circuits," *Dig., 1971 Int'l Symp. on Fault-Tolerant Computing*, pp. 26-29.June 1971.
[Shedletsky 77] Shedletsky, J.J., "Random Testing: Practicality vs. Verified Effectiveness," *Proc., The Seventh Annual Int'l Conf. on Fault-Tolerant Computing*, pp. 175-179, Los Angeles, CA June 28-30, 1977.
[Wagner 87a] Wagner, K.D., C.K. Chin, and E.J. McCluskey, "Pseudorandom Testing," *IEEE Trans. Comput.*,Vol. C-36, No. 3, pp. 332-342, March 1987.

ACKNOWLEDGEMENTS

We gratefully acknowledge David McCluskey for his assistance with this manuscript. We would also like to thank Itzhak Shperling for his helpful comments. This report was supported by the Innovative Science and Technology Office of the Strategic Defense Initiative Organization and administered through the Office of Naval Research under Contract No. N00014-85-K-0600.

END

12-87

DTIC